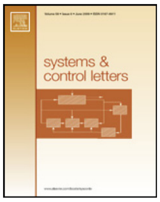
Systems & Control Letters 110 (2017) 21–28

Contents lists available at ScienceDirect

Systems & Control Letters

journal homepage: www.elsevier.com/locate/sysconle



Distributed economic model predictive control with Safeness-Index based constraints for nonlinear systems

Fahad Albalawi [a], Helen Durand [b], Panagiotis D. Christofides [b,a,*]

[a] Department of Electrical Engineering, University of California, Los Angeles, CA 90095, USA
[b] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095, USA

ARTICLE INFO

Article history:
Received 3 May 2017
Received in revised form 3 October 2017
Accepted 9 October 2017

Keywords:
Economic model predictive control
Safety
Distributed control
Process control
Nonlinear systems

ABSTRACT

In this work, sequential and iterative distributed economic model predictive control (DEMPC) architectures are developed with constraints based on a metric (termed the Safeness Index) that is indicative of the safeness of operating a process at a given state in state-space. The DEMPC's may have lower computation times than a centralized economic model predictive control (EMPC) design with Safeness Index-based constraints, without significantly limiting closed-loop economic performance, which enhances their practicality and ability to improve process operational safety. Sufficient conditions are derived under which the implementation strategies for the DEMPC's guarantee closed-loop stability.

1. Introduction

The potential for catastrophic accidents in the chemical process industries has caused chemical processes to be instrumented with various alarms [1], shut-down systems, and relief valves to prevent incidents. Recent calls for improving process safety further by handling it as a system property (e.g., [2]) have been answered by several recent works that unite control and safety within a systems framework. One of these [3] develops a metric termed the Safeness Index that indicates the relative safeness of the process state in state-space (and therefore accounts for interactions between states) and a centralized Lyapunov-based EMPC (LEMPC) scheme with constraints related to thresholds on the Safeness Index. However, a DEMPC design, in which multiple controllers optimize the same objective function and each solves for only a subset of the decision variables from the centralized EMPC design [4,5], may have a lower computation time than the centralized design, which may make it more effective for use with large-scale nonlinear industrial processes. In this work, sequential and iterative DEMPC's with Safeness Index-based constraints, and implementation strategies for each, are developed. Sufficient conditions that guarantee closed-loop stability of a nonlinear process operated under these implementation strategies are derived.

2. Preliminaries

The notations $|x|$ and x^T denote the 2-norm and transpose of a vector x, respectively. A level set of a sufficiently smooth, positive definite scalar-valued function $V(x)$ is represented by $\Omega_\rho := \{x \in R^{n_x} : V(x) \leq \rho\}$. The operator '/' denotes set subtraction, (i.e., $A/B := \{x \in R^{n_x} : x \in A, x \notin B\}$). The family of piecewise constant, right-continuous functions with time interval $\Delta > 0$ is denoted by $S(\Delta)$. A function $\alpha(\cdot) : [0, a) \to [0, \infty)$ belongs to class $\mathcal{K}$ if it is strictly increasing and continuous, and $\alpha(0) = 0$. We consider nonlinear process systems with the form:

$$\dot{x} = f(x) + \sum_{i=1}^{m} g_i(x)\bar{u}_i + b(x)w \tag{1}$$

where $x \in R^{n_x}$, $w \in R^{n_w}$ and $\bar{u}_i \in R^{n_i}$ for $i = 1, \ldots, m$, are the process state vector, disturbance vector and ith manipulated input vector, respectively. Each input vector $\bar{u}_i$ is constrained to be in a nonempty convex set $U_i := \{\bar{u}_i \in R^{n_i} : |\bar{u}_i| \leq \bar{u}_i^{\max}\}$, where $\bar{u}_i^{\max}$ is a bound on the 2-norm of $\bar{u}_i$ resulting from actuator limitations. State measurements are assumed to be available at synchronous time instants $t_k = t_0 + k\Delta$, $k = 0, 1, \ldots,$ where Δ is the sampling period and t_0 is the initial time. Bounded disturbances are considered in the sense that $w \in W := \{w \in R^{n_w} : |w| \leq \theta, \theta > 0\}$. The vector functions f, g_i, $i = 1, \ldots, m$, and b are assumed to be locally Lipschitz vector functions of their arguments. The origin is assumed to be an equilibrium point of the unforced nominal (i.e., $w(t) \equiv 0$) system (i.e., $f(0) = 0$, $g_i(0) = 0$, $i = 1, \ldots, m$, and $b(0) = 0$).

[*] Corresponding author at: Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

https://doi.org/10.1016/j.sysconle.2017.10.002
0167-6911/© 2017 Elsevier B.V. All rights reserved.

We consider systems of the form of Eq. (1) that are stabilizable in the sense that there exists a locally Lipschitz feedback control law $\bar{h}^T(x) = [\bar{h}_1(x) \ \ldots \ \bar{h}_m(x)]$ with $\bar{h}(0) = 0$ for the nominal closed-loop system of Eq. (1) that renders the origin of the nominal system asymptotically stable for all $x \in D \subseteq R^{n_x}$, where D is an open neighborhood of the origin, in the sense that there exist a sufficiently smooth Lyapunov function $V(x)$ [6] for the nominal closed-loop system and class $\mathcal{K}$ functions $\alpha_i(\cdot)$, $i = 1, 2, 3, 4$, such that the following inequalities hold for all $x \in D$:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \tag{2a}$$

$$\frac{\partial V(x)}{\partial x}(f(x) + \sum_{i=1}^{m} g_i(x)\bar{h}_i(x)) \leq -\alpha_3(|x|) \tag{2b}$$

$$\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|),\ \bar{h}_i(x) \in U_i,\ i = 1, \ldots, m \tag{2c}$$

The stability region of the closed-loop system (denoted by Ω_ρ) is taken to be a level set of the Lyapunov function within D where Eq. (2) holds. By the local Lipschitz property assumed for the vector fields $f, g_i, i = 1, \ldots, m$, and b, the smoothness of the Lyapunov function $V(x)$, and the boundedness of $\bar{u}_i$, $i = 1, \ldots, m$, and w, there exist positive constants $M, L_x, L_{\bar{u}_i}$, $i = 1, \ldots, m$, and L_w such that

$$\left|f(x) + \sum_{i=1}^{m} g_i(x)\bar{u}_i + b(x)w\right| \leq M \tag{3}$$

$$\left|\frac{\partial V}{\partial x}f(x) - \frac{\partial V}{\partial x}f(x')\right| \leq L_x\left|x - x'\right|,\quad \left|\frac{\partial V}{\partial x}b(x)\right| \leq L_w \tag{4}$$

$$\left|\frac{\partial V}{\partial x}g_i(x) - \frac{\partial V}{\partial x}g_i(x')\right| \leq L_{\bar{u}_i}\left|x - x'\right|,\ i = 1, \ldots, m \tag{5}$$

for all $x, x' \in \Omega_\rho, \bar{u}_i \in U_i, i = 1, \ldots, m$, and $w \in W$.

3. Distributed Safeness Index-based LEMPC

A centralized LEMPC design was developed in [3] (i.e., one optimization problem is solved to determine the values of all $\bar{u}_i$, $i = 1, \ldots, m$) with constraints requiring the value of the Safeness Index (which is functionally dependent on the state vector x and is therefore denoted by $S(x)$) evaluated along the predicted state trajectory under the LEMPC to be no greater than a threshold value S_{TH} to seek to prevent the process state from approaching unsafe operating conditions. The computation time required to solve this centralized Safeness Index-based LEMPC may be significant with the process model and constraints of a large-scale industrial nonlinear process system with tens or hundreds of inputs. Therefore, the problem may not be solved to optimality within a short sampling period, which prevents the optimization problem from being solved frequently with new state measurements. However, frequent feedback of the process state can be beneficial for enhancing process safety under this control design because the region where $S(x) \leq S_{TH}$ (the safety zone) is not necessarily an invariant set under the Safeness Index-based LEMPC design, and the controller is made aware that the state has exited the safety zone (so that it can compute control actions guaranteed to drive the state back into the safety zone in finite time) through feedback of the process state [3]. Moreover, this LEMPC design may be applied in practice to processes for which the upper bound on the disturbance is estimated but not known (though that is not the theoretical consideration in this work), and in such cases, more frequent feedback may aid in preventing the closed-loop state from exiting the safety zone during a sampling period if a disturbance potentially greater than the expected bound affects the process. To obtain Safeness Index-based controllers with reduced computation time (allowing more frequent feedback) compared to the centralized design, this work develops two distributed (sequential and iterative) Safeness Index-based LEMPC designs.

3.1. Safeness Index-based Sequential DLEMPC

The first distributed control scheme considered is a sequential Safeness Index-based DLEMPC (termed Safeness Index-S-DLEMPC) design where each of m controllers solves for a different subset of the set of all control actions. The jth controller solves for the n_j control actions in vector $\bar{u}_j$ out of the total $n_{tot} = \sum_{i=1}^{m} n_i$ available control actions while it assumes values of the remaining $n_{tot} - n_j$ manipulated inputs. In the Safeness Index-S-DLEMPC design, the m controllers form a hierarchy connected using a one-directional communication network and are evaluated in sequence (i.e., the first LEMPC in the hierarchy calculates $\bar{u}_1$, the second LEMPC receives the computed value of $\bar{u}_1$ and calculates $\bar{u}_2$, and so on). The jth controller, $j \in \{1, \ldots, m\}$, in the hierarchy (Safeness Index-S-DLEMPC j) solves only for $\bar{u}_j$. It assumes that $\bar{u}_z, z = 1, \ldots, j-1$, are the optimal values of these control actions from the controllers higher up in the hierarchy, and assumes that $\bar{u}_z = \bar{h}_z(\tilde{x}(t_q)), \forall\ t \in [t_q, t_{q+1}), q = k, \ldots, k+N-1$, for $z = j+1, \ldots, m$. The jth Safeness Index-S-DLEMPC solves the following optimization problem for the input trajectory $\bar{u}_j(t)$ over the prediction horizon $N\Delta$:

$$\max_{\bar{u}_j \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau))d\tau \tag{6a}$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t))\bar{u}_i(t) \tag{6b}$$

$$\bar{u}_j(t) \in U_j,\ \forall\ t \in [t_k, t_{k+N}) \tag{6c}$$

$$\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q})),\ r = j+1, \ldots, m, \quad \forall\ t \in [t_{k+q}, t_{k+q+1}),\ q = 0, \ldots, N-1 \tag{6d}$$

$$\bar{u}_p(t) = \bar{u}_p^*(t|t_k), \qquad p = 1, \ldots, j-1,\ t \in [t_k, t_{k+N}) \tag{6e}$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{6f}$$

$$V(\tilde{x}^j(t)) \leq \rho_e,\ \forall\ t \in [t_k, t_{k+N}) \quad \text{if } x(t_k) \in \Omega_{\rho_e} \tag{6g}$$

$$S(\tilde{x}^j(t)) \leq S_{TH},\ \forall\ t \in [t_k, t_{k+N}) \quad \text{if } S(x(t_k)) \leq S_{TH} \tag{6h}$$

$$\frac{\partial V(x(t_k))}{\partial x}(\sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i(t_k)) \leq \frac{\partial V(x(t_k))}{\partial x}(\sum_{i=1}^{m} g_i(x(t_k))\bar{h}_i(x(t_k))), \quad \text{if } x(t_k) \in \Omega_\rho/\Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH} \tag{6i}$$

where $\tilde{x}^j(t)$ denotes the predicted state trajectory under Safeness Index-S-DLEMPC j. This control scheme maximizes the time integral of an economics-based stage cost $L_e(x, \bar{u}_1, \ldots, \bar{u}_m)$ (Eq. (6a)), subject to input constraints (Eq. (6c)) and a nominal process model (Eq. (6b)) initialized with a state measurement at the current sampling time t_k (Eq. (6f)). The notation t_s denotes the time after which it is desired to apply the constraint of Eq. (6i). The predicted state trajectory $\tilde{x}^j(t)$ is maintained within Ω_{ρ_e} throughout the prediction horizon by the constraint of Eq. (6g) when $x(t_k) \in \Omega_{\rho_e}$. The region Ω_{ρ_e} is chosen such that if the measured state $x(t_k)$ is within Ω_{ρ_e}, then $x(t_{k+1})$ is still within Ω_{ρ_e}, even in the presence of uncertainty. The constraint of Eq. (6h) maintains the predicted closed-loop state within the safety zone throughout the prediction horizon when $S(x(t_k)) \leq S_{TH}$. The safety zone is assumed to contain the origin of the system of Eq. (1) in its interior. The contractive constraint of Eq. (6i) guarantees that feasible control actions will decrease the value of the Lyapunov function between t_k and t_{k+1} when this constraint is applied (i.e., $x(t_k) \in \Omega_\rho/\Omega_{\rho e}$, $t_k > t_s$, or $S(x(t_k)) > S_{TH}$). Because the activation conditions of the constraints of Eqs. (6g)–(6i) are different, more than one of these constraints may be activated simultaneously (see also [3]). The constraint of Eq. (6e) sets the trajectory of each $\bar{u}_p$, $p = 1, \dots, j-1$, to the optimal trajectory (denoted by $\bar{u}_p^*(t|t_k)$, $t \in [t_k, t_{k+N})$) calculated by Safeness Index-S-DLEMPC p, $p = 1, \dots, j-1$. The values of the inputs $\bar{u}_r$, $r = j+1, \dots, m$, that will be calculated by Safeness Index-S-DLEMPC's later in the sequence of m controllers are set by the constraint of Eq. (6d) to the corresponding elements of $\bar{h}(x)$ applied in a sample-and-hold fashion.

The manner in which the n_{tot} inputs are partitioned between the various $\bar{u}_j$ and the order in which the various $\bar{u}_j$ are computed in the hierarchy of distributed controllers can impact whether each of the m controllers in the hierarchy is feasible. Specifically, when Eq. (6h) is not applied (i.e., $S(x(t_k)) > S_{TH}$), $\bar{u}_j = \bar{h}_j(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \dots, k+N-1$, is a feasible control action for Safeness Index-S-DLEMPC j. However, the region where $S(x) \le S_{TH}$ is not required to take a specific shape (e.g., it is not required to be a Lyapunov level set), so when Eq. (6h) is applied, there is no guarantee that any control action within the input bounds can satisfy this constraint (whether or not constraints such as Eqs. (6g) and/or (6i) are simultaneously applied). This means that the jth Safeness Index-S-DLEMPC will have a feasible solution when the constraint of Eq. (6h) is applied only if there exists a $\bar{u}_j$ that, when $\bar{u}_p(t) = \bar{u}_p^*(t|t_k)$, $p = 1, \dots, j-1$, $t \in [t_k, t_{k+N})$, and $\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q}))$, $r = j+1, \dots, m$, $\forall\, t \in [t_{k+q}, t_{k+q+1})$, $q = 0, \dots, N-1$, the state predictions are maintained within the safety zone. Furthermore, if the control actions calculated by Safeness Index-S-DLEMPC 1 ensure that $S(\tilde{x}^1) \le S_{TH}$ throughout the prediction horizon (i.e., Safeness Index-S-DLEMPC 1 is feasible even when Eq. (6h) is applied), then Safeness Index-S-DLEMPC 2 to Safeness Index-S-DLEMPC m will be feasible as well because a feasible solution to Safeness Index-S-DLEMPC j is a feasible solution to Safeness Index-S-DLEMPC $j+1$. Hence, grouping inputs that have a large effect on the magnitude of $S(x)$ (and thus provide significant flexibility for adjusting its value throughout the prediction horizon to seek to maintain the state predictions within the safety zone) together within $\bar{u}_1$ may enable the constraint of Eq. (6h) to be feasible more regularly in Safeness Index-S-DLEMPC 1 than if inputs with less impact on $S(x)$ were computed by this controller. This would allow the set of m distributed controllers to be feasible more regularly as well (since all are feasible if Safeness Index-S-DLEMPC 1 is feasible). Furthermore, other process constraints beyond those presented in Eq. (6) may be added to the Safeness Index-S-DLEMPC's (e.g., constraints on the time-averaged value of certain inputs or products of inputs due to physical constraints on the process such as available reactant), and input partitioning may impact feasibility of these constraints as well. For example, if a constraint on the product of two inputs is present, it may be desirable to solve for both inputs in the same Safeness Index-S-DLEMPC if it is likely that the constraint will be infeasible if such flexibility in satisfying the constraint is not provided. Process economics may be impacted by the manner in which the inputs are partitioned (e.g., as the number of control actions n_j determined by Safeness Index-S-DLEMPC j is decreased due to an increasing magnitude of m, Safeness Index-S-DLEMPC j may have less flexibility to maximize process economic performance). Computation time is also affected by input partitioning (e.g., it may increase for Safeness Index-S-DLEMPC j if n_j is increased to provide the LEMPC with greater flexibility in control action selection for feasibility and/or economics reasons). Thus, an appropriate partitioning of inputs may be based on trade-offs between feasibility, economics, and computation time considerations. This approach for partitioning inputs may be complemented by other methods of input partitioning (see, e.g., [4,7]), though the partitions resulting from alternative methods should be evaluated from the feasibility standpoint discussed before being used.

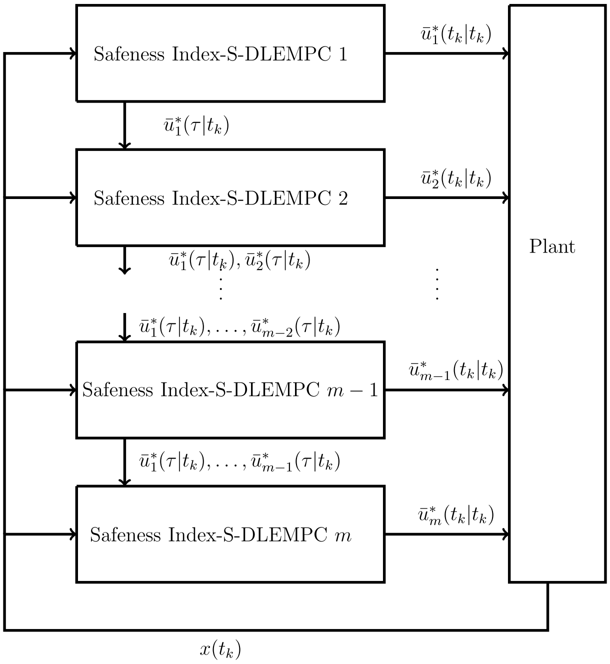

Safeness Index-S-DLEMPC 1
$\bar{u}_1^*(t_k|t_k)$
$\bar{u}_1^*(\tau|t_k)$
Safeness Index-S-DLEMPC 2
$\bar{u}_2^*(t_k|t_k)$
Plant
$\bar{u}_1^*(\tau|t_k), \bar{u}_2^*(\tau|t_k)$
$\bar{u}_1^*(\tau|t_k), \dots, \bar{u}_{m-2}^*(\tau|t_k)$
Safeness Index-S-DLEMPC $m-1$
$\bar{u}_{m-1}^*(t_k|t_k)$
$\bar{u}_1^*(\tau|t_k), \dots, \bar{u}_{m-1}^*(\tau|t_k)$
Safeness Index-S-DLEMPC m
$\bar{u}_m^*(t_k|t_k)$
$x(t_k)$

Fig. 1. Block diagram of the Safeness Index-S-DLEMPC scheme.

A schematic of the Safeness Index-S-DLEMPC architecture is depicted in Fig. 1. An implementation issue for the Safeness Index-S-DLEMPC design is that, when Safeness Index-S-DLEMPC 1 is infeasible when the constraint of Eq. (6h) is applied, no feasible solution to Safeness Index-S-DLEMPC 1 is available to be sent to Safeness Index-S-DLEMPC 2 to m. Safeness Index-S-DLEMPC 2 to m cannot then be solved to obtain $u_i^*(t_k|t_k)$, $i = 1, \dots, m$, to apply to the process; in such cases, we require that the explicit stabilizing controller $\bar{h}_i(x(t_k))$, $i = 1, \dots, m$, be applied to the plant because $\bar{h}(x(t_k))$ is guaranteed to maintain the closed-loop state in Ω_ρ throughout a sampling period [8]. This implementation strategy for the Safeness Index-S-DLEMPC design is summarized as follows:

1. At t_k, the m Safeness Index-S-DLEMPC's receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2.
2. Solve Safeness Index-S-DLEMPC 1. If the Safeness Index-S-DLEMPC 1 optimization problem is feasible, go to Step 2a. Else, go to Step 2b.
    (a) Safeness Index-S-DLEMPC 1 sends $\bar{u}_1^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, to Safeness Index-S-DLEMPC 2. Go to Step 3 ($j = 2$).
    (b) Apply $\bar{u}_i(t_k) = \bar{h}_i(x(t_k))$, $i = 1, \dots, m$, to the plant. Go to Step 6.
3. Solve Safeness Index-S-DLEMPC j. If $j < m$, go to Step 4. If $j = m$, go to Step 5.
4. Send $\bar{u}_p^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, $p = 1, \dots, j$, to Safeness Index-S-DLEMPC $j+1$. Go to Step 3 ($j \leftarrow j+1$).
5. The m Safeness Index-S-DLEMPC's send the optimal solutions $u_i^*(t_k|t_k)$, $i = 1, \dots, m$, for the first sampling period of the prediction horizon to the actuators to be implemented on the process. Go to Step 6.
6. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

Remark 1. The partitioning of the inputs based on feasibility is not intended to make the m Safeness Index-S-DLEMPC's feasible at each sampling time (e.g., when the centralized Safeness Index-based LEMPC would be infeasible at t_k because the safety zone is not necessarily a forward invariant set, there is no partitioning of the inputs that would be able to make Safeness Index-S-DLEMPC 1 to m feasible). Appropriate partitioning is intended to prevent the distributed controllers from frequently becoming infeasible when the centralized design would not have been.

3.1.1. Feasibility and closed-loop stability analysis for the Safeness Index-S-DLEMPC implementation strategy

To prove closed-loop stability of a nonlinear process operated under the Safeness Index-S-DLEMPC implementation strategy, we introduce three propositions which, respectively, illustrate the closed-loop stability properties of the Lyapunov-based controller used for the Safeness Index-S-DLEMPC constraint design, bound the norm of the difference between the trajectories of the nominal and perturbed (i.e., $w(t) \not\equiv 0$) systems when initiated from the same initial condition, and bound the difference in the Lyapunov function value at different locations in the stability region.

Proposition 1 (*c.f.* [8]). *Consider the trajectory $\hat{x}(t)$ of the system of Eq. (1) in closed-loop under a controller $\bar{h}(x)$, which satisfies the conditions of Eq. (2), obtained by solving recursively:*

$$\dot{\hat{x}}(t) = f(\hat{x}(t)) + \sum_{i=1}^{m} g_i(\hat{x}(t))\bar{h}_i(\hat{x}(t_k)) + b(\hat{x}(t))w(t) \tag{7}$$

where $t \in [t_k, t_{k+1})$ with $k = 0, 1, \ldots$. Let $\Delta, \epsilon_w > 0$ and $\rho > \rho_s > 0$ satisfy:

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + (L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{\max})M\Delta + L_w\theta \le -\epsilon_w/\Delta. \tag{8}$$

Then, if $\hat{x}(t_0) \in \Omega_\rho$ and $\rho_{\min} < \rho$ where

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \le \rho_s\}, \tag{9}$$

the following inequality holds:

$$V(\hat{x}(t_k)) \le \max\{V(\hat{x}(t_0)) - k\epsilon_w, \rho_{\min}\}. \tag{10}$$

Proposition 2 (*c.f.* [9,10]). *Consider the systems*

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t)) + \sum_{i=1}^{m} g_i(x_a(t))\bar{u}_i(t) + b(x_a(t))w(t) \\ \dot{x}_b(t) &= f(x_b(t)) + \sum_{i=1}^{m} g_i(x_b(t))\bar{u}_i(t) \end{aligned} \tag{11}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_\rho$. There exists a $\mathcal{K}$ function $f_W(\cdot)$ such that

$$|x_a(t) - x_b(t)| \le f_W(t - t_0), \tag{12}$$

for all $x_a(t), x_b(t) \in \Omega_\rho$ and all $w(t) \in W$ with

$$f_W(\tau) = \frac{L'_w\theta}{L'_x}(e^{L'_x\tau} - 1). \tag{13}$$

where L'_w and L'_x are positive constants.

Proposition 3 (*c.f.* [9,10]). *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. (1). There exists a quadratic function $f_V(\cdot)$ such that*

$$V(x) \le V(x') + f_V(|x - x'|) \tag{14}$$

for all $x, x' \in \Omega_\rho$ with

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{15}$$

where M_v is a positive constant.

We note that $\rho_{\min}$ in Proposition 1 is defined without reference to a specific controller such as $\bar{h}(x)$, but rather as the maximum value that $V(x)$ can take in a time period Δ if $V(x(t)) \le \rho_s$ at the beginning of this time period, given Δ and the constraints. Proposition 1 guarantees that with a sufficiently small sampling period and bound on the disturbance (i.e., Eq. (8) holds), the magnitude of $V(x)$ decreases throughout a sampling period for the system of Eq. (1) under $\bar{h}(x)$ when $\hat{x}(t_k) \in \Omega_\rho/\Omega_{\rho_s}$, and when $\hat{x}(t_k) \in \Omega_{\rho_s}$, then $\hat{x}(t) \in \Omega_{\rho_{\min}}, \forall\, t \in [t_k, t_{k+1})$.

Theorem 1 below provides sufficient conditions which guarantee closed-loop stability of the system of Eq. (1) under the Safeness Index-S-DLEMPC implementation strategy.

Theorem 1. *Consider the system of Eq. (1) in closed-loop under the implementation strategy (Steps 1–6) of the Safeness Index-S-DLEMPC based on a controller $\bar{h}(x)$ that satisfies the conditions of Eq. (2). Let $\epsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ satisfy*

$$\rho_e \le \rho - f_V(f_W(\Delta)) \tag{16}$$

and Eq. (8). If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \le \rho_e$ and $N \ge 1$ where $\rho_{\min}$ is defined as in Eq. (9) and where the compact set $\Omega_{\rho_{\min}}$ satisfies

$$\Omega_{\rho_{\min}} \subseteq \{x \in \Omega_\rho \; : \; S(x) \le S_{TH}\}, \tag{17}$$

then the closed-loop state $x(t)$ of Eq. (1) is guaranteed to enter the safety zone in finite time when $x(t_0) \in \Omega_\rho$, to be bounded within Ω_ρ at all times, and to be ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof. The proof of Theorem 1 is given in two parts. The first part is the proof of the existence of an input trajectory with characterizable properties for the process of Eq. (1) operated under Steps 1–6 of the Safeness Index-S-DLEMPC implementation strategy when $x(t_0) \in \Omega_\rho$. The second part proves the three results of Theorem 1 given these characterizable properties.

Part 1: Based on the implementation strategy of the Safeness Index-S-DLEMPC, in a given sampling period, either: (1) Safeness Index-S-DLEMPC 1 is a feasible optimization problem and $\bar{u}_1^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, is communicated to Safeness Index-S-DLEMPC 2, or (2) Safeness Index-S-DLEMPC 1 is not feasible and $\bar{h}_i(x(t_k))$ for $i = 1, \ldots, m$, is applied to the process for $t \in [t_k, t_{k+1})$. In the case that Safeness Index-S-DLEMPC 1 is feasible, Safeness Index-S-DLEMPC's 2 to m are guaranteed to be feasible. This is because if Safeness Index-S-DLEMPC j is feasible with the input trajectories defined by $\bar{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $\bar{u}_p(t) = \bar{u}_p^*(t|t_k)$, $p = 1, \ldots, j-1$, $t \in [t_k, t_{k+N})$, and $\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q}))$, $r = j+1, \ldots, m$, $\forall\, t \in [t_{k+q}, t_{k+q+1})$, $q = 0, \ldots, N-1$, then in Safeness Index-S-DLEMPC $j+1$, which solves for $\bar{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, but sets the other inputs according to the constraints of Eqs. (6d)–(6e) (which forces all inputs except $\bar{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, to take the same values as they had in the feasible solution returned by Safeness Index-S-DLEMPC j), the trajectory of $\bar{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, that was feasible for Safeness Index-S-DLEMPC j (i.e., $\bar{u}_{j+1}^*(t|t_k) = \bar{h}_{j+1}(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$) is feasible for Safeness Index-S-DLEMPC $j+1$. When $\bar{u}_{j+1}^*(t|t_k) = \bar{h}_{j+1}(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, is applied with the input trajectories of Eqs. (6d)–(6e), the state predictions of Eq. (6b) for Safeness Index-S-DLEMPC's j and $j+1$ are initiated from the same initial condition (Eq. (6f)) and have the same input trajectories. We assume that the local Lipschitz property for vector functions f, g_i, $i = 1, \ldots, m$, and b allows them to be constructed such that since $x(t) \in \Omega_\rho$ for all times (as will be demonstrated in Part 2 of this proof), Eq. (6b) in Safeness Index-S-DLEMPC's j and $j+1$ has the same unique solution throughout the prediction horizon when the same input trajectories are applied [6]; therefore, if such trajectories meet the constraints of Eqs. (6g)–(6i) in Safeness Index-S-DLEMPC j, they will also meet them in Safeness Index-S-DLEMPC $j+1$. The only constraint in Eq. (6) that is enforced in Safeness Index-S-DLEMPC $j+1$ that is not enforced in Safeness Index-S-DLEMPC j is Eq. (6c) (in Safeness Index-S-DLEMPC j, it is enforced on $\bar{u}_j$, whereas in Safeness Index-S-DLEMPC $j+1$, it is enforced on $\bar{u}_{j+1}$). By Eq. (2), however, $\bar{u}^*_{j+1}(t|t_k) = \bar{h}_{j+1}(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, satisfies this constraint as well, showing that this trajectory fully satisfies all constraints of Safeness Index-S-DLEMPC $j+1$ if Safeness Index-S-DLEMPC j was feasible. Because Safeness Index-S-DLEMPC 1 is feasible, Safeness Index-S-DLEMPC's 2 to m are therefore feasible by induction. When a feasible solution to Safeness Index-S-DLEMPC's 1 to m is obtained, Eqs. (6b)–(6i) are satisfied in Safeness Index-S-DLEMPC m for the set of implemented control actions $\bar{u}^*_i(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, and thus the set of implemented control actions has characterizable properties. When Safeness Index-S-DLEMPC 1 is not feasible and $\bar{h}(x(t_k))$ is applied, the conditions of Proposition 1 hold. Thus, the control actions applied to the process according to the Safeness Index-S-DLEMPC implementation strategy throughout any sampling period have characterizable properties that can be used to analyze closed-loop stability of a nonlinear process under these control actions.

Part 2: We now prove the results of Theorem 1. To prove that if $S(x(t_k)) > S_{TH}$ and $x(t_0) \in \Omega_\rho$, then the Safeness Index-S-DLEMPC implementation strategy will drive the closed-loop state into the safety zone in finite time, we demonstrate that either a feasible solution to all m distributed controllers of the Safeness Index-S-DLEMPC design or $\bar{h}(x(t_k))$ will drive the closed-loop state toward the set $\Omega_{\rho_{\min}}$ (which is within the safety zone from Eq. (17)) throughout a given sampling period. When all m Safeness Index-S-DLEMPC's are feasible at a given sampling time (which follows if Safeness Index-S-DLEMPC 1 is feasible), the set of control actions $\bar{u}^*_i(t_k|t_k)$, $i = 1, \ldots, m$, that are applied to the process satisfy the constraints of Safeness Index-S-DLEMPC m (the last controller in the hierarchy). Specifically, when $S(x(t_k)) > S_{TH}$, from the contractive constraint of Eqs. (6i) and (2b), we obtain:

$$\frac{\partial V(x(t_k))}{\partial x}\left(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{u}^*_i(t_k|t_k)\right)$$
$$\leq \frac{\partial V(x(t_k))}{\partial x}\left(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{h}_i(x(t_k))\right) \tag{18a}$$
$$\leq -\alpha_3(|x(t_k)|) \tag{18b}$$

The time derivative of the Lyapunov function along the state trajectory $x(t)$ under $\bar{u}^*_i(t_k|t_k)$, $i = 1, \ldots, m$, for $t \in [t_k, t_{k+1})$, is:

$$\dot{V}(x(t)) = \frac{\partial V(x(t))}{\partial x}\Bigg(f(x(t)) + \sum_{i=1}^{m} g_i(x(t))\bar{u}^*_i(t_k|t_k) + b(x(t))w(t)\Bigg) \tag{19}$$

Adding and subtracting $\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{u}^*_i(t_k|t_k))$ to/from Eq. (19), we obtain the following inequality by utilizing Eq. (18), the Lipschitz properties in Eqs. (4)–(5), and the disturbance bound $|w| \leq \theta$:

$$\dot{V}(x(t)) \leq -\alpha_3(|x(t_k)|) + \Bigg(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}^*_i(t_k|t_k)\Bigg)|x(t) - x(t_k)| + L_w\theta \tag{20}$$

From the continuity of $x(t)$ and Eq. (3), the following bound holds for all $t \in [t_k, t_{k+1})$:

$$|x(t) - x(t_k)| \leq M\Delta \tag{21}$$

Because $S(x(t_k)) > S_{TH}$, it follows from Eqs. (9) and (17) that $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$. In addition, since Eqs. (20)–(21) and the bounds on $\bar{u}_i$, $i = 1, \ldots, m$, also hold, the following bound on $\dot{V}(x(t))$ can be written for $t \in [t_k, t_{k+1})$:

$$\dot{V}(x(t)) \leq -\alpha_3(\alpha_2^{-1}(\rho_s)) + \left(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{\max}\right)M\Delta + L_w\theta \tag{22}$$

When Eq. (8) is satisfied, there exists $\epsilon_w > 0$ such that the following inequality holds for $S(x(t_k)) > S_{TH}$:

$$\dot{V}(x(t)) \leq -\epsilon_w/\Delta \quad \forall\, t \in [t_k, t_{k+1}) \tag{23}$$

Integrating the bound of Eq. (23) on $t \in [t_k, t_{k+1})$ gives:

$$V(x(t_{k+1})) \leq V(x(t_k)) - \epsilon_w \tag{24a}$$
$$V(x(t)) \leq V(x(t_k)), \quad \forall\, t \in [t_k, t_{k+1}) \tag{24b}$$

whenever $S(x(t_k)) > S_{TH}$ and the m Safeness Index-S-DLEMPC's are feasible. When Safeness Index-S-DLEMPC 1 has no feasible solution and $x(t_0) \in \Omega_\rho$, then $\bar{h}(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$, which will decrease the value of the Lyapunov function between t_k and t_{k+1} according to Proposition 1. Therefore, regardless of whether $\bar{u}^*_i(t_k|t_k)$, $i = 1, \ldots, m$, or $\bar{h}(x(t_k))$ is implemented throughout a given sampling period when $S(x(t_k)) > S_{TH}$, $V(x(t_{k+1})) < V(x(t_k))$ and the sequence of control actions implemented until $S(x(t_k)) \leq S_{TH}$ will thus drive the closed-loop state into Lyapunov level sets with a smaller upper bound on the Lyapunov function. This will eventually drive the state into the safety zone, because the control actions will drive the state toward $\Omega_{\rho_{\min}}$ throughout every sampling period and thus into $\Omega_{\rho_{\min}}$ if $S(x(t_k))$ is greater than S_{TH} at every sampling time until $x(t_k) \in \Omega_{\rho_{\min}}$ (the state is within the safety zone after it is within $\Omega_{\rho_{\min}}$ from Eq. (17), regardless of the shape of the safety zone).

To prove that $x(t) \in \Omega_\rho$, $\forall\ t \in [t_0, \infty)$, when $x(t_0) \in \Omega_\rho$ for a process operated under the Safeness Index-S-DLEMPC implementation strategy, we begin by demonstrating that if $x(t_k) \in \Omega_\rho$, then $x(t) \in \Omega_\rho, \forall\, t \in [t_k, t_{k+1})$, both in the case that a feasible solution of the Safeness Index-S-DLEMPC design is applied to the process and in the case that $\bar{h}(x(t_k))$ is instead applied for $t \in [t_k, t_{k+1})$. When Safeness Index-S-DLEMPC 1 is feasible and $x(t_k) \in \Omega_{\rho_e}$ such that the constraint of Eq. (6g) is applied and satisfied by the solution of Safeness Index-S-DLEMPC m under the implemented control actions $\bar{u}^*_i(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, then $\tilde{x}^m(t) \in \Omega_{\rho_e}$ for $t \in [t_k, t_{k+1})$. From Propositions 2 and 3, and considering that the maximum value of $t - t_k$ for $t \in [t_k, t_{k+1})$ is Δ, we have that

$$V(x(t)) \leq V(\tilde{x}^m(t)) + f_V(f_W(\Delta)) \tag{25}$$

for $t \in [t_k, t_{k+1})$. Since $V(\tilde{x}^m(t)) \leq \rho_e$ for $t \in [t_k, t_{k+1})$ and Eq. (16) holds, we conclude that $x(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. If $x(t_k) \in \Omega_\rho/\Omega_{\rho_e}$ (or $S(x(t_k)) > S_{TH}$), then Eq. (6i) is active and Eqs. (24a)–(24b) hold, preventing the closed-loop state from leaving Ω_ρ in a sampling period. When Safeness Index-S-DLEMPC 1 is not feasible, then $\bar{h}(x(t_k))$ will be applied for $t \in [t_k, t_{k+1})$, in which case Proposition 1 holds. A similar series of steps to those performed in Eqs. (18)–(24) can be performed when Proposition 1 holds, with the result that Eqs. (24a)–(24b) hold when Proposition 1 holds and therefore $x(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. Since throughout each sampling period, a feasible solution to the m Safeness Index-S-DLEMPC's or $\bar{h}(x(t_k))$ maintains the closed-loop state within Ω_ρ, the sequence of control actions generated throughout time by applying either the Safeness Index-S-DLEMPC m solution or $\bar{h}(x(t_k))$

at each sampling time according to the Safeness Index-S-DLEMPC implementation strategy maintains the closed-loop state in Ω_ρ.

Finally, the closed-loop state under the Safeness Index-S-DLEMPC implementation strategy is ultimately bounded in $\Omega_{\rho_{\min}}$ when $t_k > t_s$ because when $t_k > t_s$, either a feasible solution to the m Safeness Index-S-DLEMPC's that had Eq. (6i) applied is implemented for the process, or $\bar{h}(x(t_k))$ is implemented. In both cases, Eqs. (24a)–(24b) hold and the Lyapunov function value decreases until the closed-loop state enters $\Omega_{\rho_{\min}}$ in finite time. After it enters $\Omega_{\rho_{\min}}$, it cannot come out due to the definition of $\Omega_{\rho_{\min}}$ in Eq. (9).

3.2. Safeness Index-based Iterative DLEMPC

In this section, we develop an iterative Safeness Index-based DLEMPC paradigm (Safeness Index-I-DLEMPC). In the iterative control design, each of the m controllers calculates a control action simultaneously. The jth controller solves for $\bar{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $j = 1, \ldots, m$, and assumes that the control actions for which it does not solve ($\bar{u}_z$, $z \in \{1, \ldots, m\}$, $z \neq j$) are set to $\bar{h}_z(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$. After the solution for each controller is obtained, either this solution is applied to the process or is provided to (exchanged with) the other $m-1$ Safeness Index-I-DLEMPC's and each of the m controllers is then re-solved assuming that the control actions for which it does not solve are set to the values $\bar{u}_z^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$, that have just been exchanged. Each re-solution of all m optimization problems is called an iteration. The number of iterations of the Safeness Index-I-DLEMPC is an integer $c \in [1, \infty)$, where $c = 1$ corresponds to the case that the m controllers have not yet exchanged solutions. The termination condition for the iterations of the Safeness Index-I-DLEMPC design can be chosen in various ways; for example, a fixed number of iterations may be selected after which the solution of all m controllers is implemented on the process at t_k and the optimization problems no longer exchange solutions. Another consideration to prevent further iterations at t_k is to terminate the optimization problem when the value of the objective function evaluated using the predicted nominal process state trajectories when $\bar{u}_i(t) = \bar{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, at iteration c shows no improvement compared to iteration $c-1$ or improves by no more than a tolerance ϵ. However, even with a termination condition based on the objective function, there is no guarantee that the economic performance of a nonlinear process under the Safeness Index-I-DLEMPC design will be comparable to that of the process under the centralized Safeness Index-based LEMPC since the manipulated inputs in the Safeness Index-I-DLEMPC are calculated by different controllers. The block diagram in Fig. 2 shows the Safeness Index-I-DLEMPC, where the solution to Safeness Index-I-DLEMPC j at time t_k at iteration c is denoted by $\bar{u}_{j,c}^*(t|t_k)$, $t \in [t_k, t_{k+N})$. The formulation of the jth Safeness Index-I-DLEMPC is:

$$\max_{\bar{u}_j \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau))d\tau \tag{26a}$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t))\bar{u}_i(t) \tag{26b}$$

$$\bar{u}_j(t) \in U_j, \ \ \forall\ t \in [t_k, t_{k+N}) \tag{26c}$$

$$\begin{aligned}\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+r})), z \in \{1, \ldots, m\},\\ z \neq j, \ \ \forall\ t \in [t_{k+r}, t_{k+r+1}),\\ r = 0, \ldots, N-1, \ c = 1\end{aligned} \tag{26d}$$

$$\begin{aligned}\bar{u}_z(t) = \bar{u}_{z,c-1}^*(t|t_k), \ z \in \{1, \ldots, m\},\\ z \neq j, \ t \in [t_k, t_{k+N}), \ c \geq 2\end{aligned} \tag{26e}$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{26f}$$

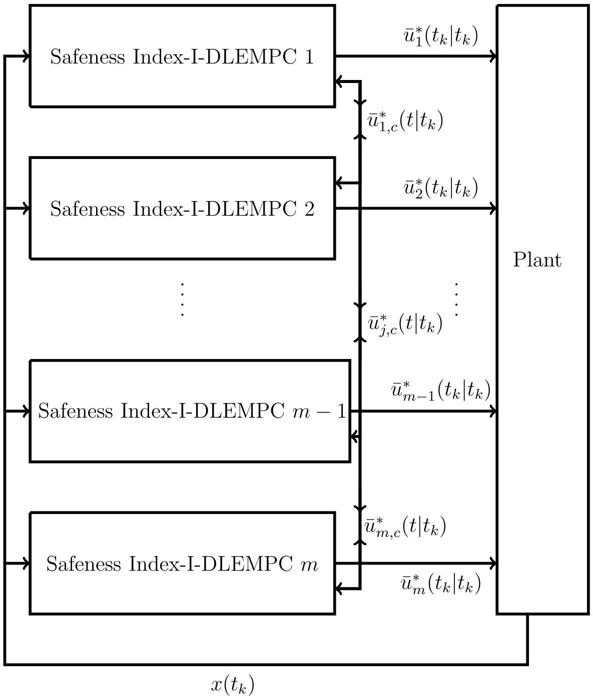


Fig. 2. Block diagram of the Safeness Index-I-DLEMPC scheme.

$$\begin{aligned}V(\tilde{x}^j(t)) \leq \rho_e, \ \ \forall\ t \in [t_k, t_{k+N})\\ \text{if } x(t_k) \in \Omega_{\rho_e}\end{aligned} \tag{26g}$$

$$\begin{aligned}S(\tilde{x}^j(t)) \leq S_{TH}, \ \ \forall\ t \in [t_k, t_{k+N})\\ \text{if } S(x(t_k)) \leq S_{TH}\end{aligned} \tag{26h}$$

$$\begin{aligned}&\frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{u}_j(t_k)\\ &\quad \leq \frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{h}_j(x(t_k)),\\ &\text{if } x(t_k) \in \Omega_\rho/\Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH}\end{aligned} \tag{26i}$$

The notations of Eqs. (26a)–(26c) and Eqs. (26f)–(26h) follow that in Eq. (6). Eq. (26d) is applied when $c = 1$ (i.e., no iteration has yet been performed at t_k) and assumes $\bar{u}_z(t)$ is $\bar{h}_z(x)$, $z \neq j$, implemented in sample-and-hold throughout the prediction horizon. Eq. (26e) is applied if $c > 1$ and sets $\bar{u}_z(t)$, $z \in \{1, \ldots, m\}$, where $z \neq j$, to the optimal solutions obtained from all Safeness Index-I-DLEMPC's except the jth at the prior iteration. Unlike the constraint of Eq. (6i), in which all inputs appear, the contractive constraint of Eq. (26i) only constrains the decision variable $\bar{u}_j(t_k)$.

To obtain a solution to the Safeness Index-I-DLEMPC design at t_k, all m Safeness Index-I-DLEMPC's must be feasible simultaneously. It may be more likely for all m controllers to be feasible at t_k when Eq. (26h) is applied if each vector $\bar{u}_i$, $i = 1, \ldots, m$, contains control actions that have a significant impact on $S(x)$ and therefore may give each of the m distributed controllers more flexibility to satisfy Eq. (26h). For some processes, feasibility of the m Safeness Index-I-DLEMPC's for several iterations may improve process economic performance because the controllers can exchange solutions and re-solve Eq. (26) to attempt to improve process economic performance only if the solutions of all m controllers at the prior iteration are feasible. Unlike the computation time of the Safeness Index-S-DLEMPC, which is equal to the summation of the computation times of each of the m controllers, the computation time of the iterative control architecture (at one iteration) is equal to the maximum computation time among all m Safeness Index-I-DLEMPC's (the sum of the computation times of all iterations performed is the total computation time of the iterative architecture). This indicates that increasing the number of distributed controllers (i.e., increasing m) may improve the computation time compared to using a smaller m because it parallelizes the computations more significantly. As noted in Section 3.1, constraints beyond those noted in Eq. (26) may be required to be satisfied by the process and may affect the input partitioning. Therefore, tradeoffs between feasibility, computation time, and economic performance may affect input partitioning for the Safeness Index-I-DLEMPC design.

The solutions of the m Safeness Index-I-DLEMPC's are calculated independently, with each controller assuming different values of $\bar{u}_z$, $z \in \{1, \ldots, m\}$ but $z \neq j$, than are used by the other controllers (e.g., Safeness Index-I-DLEMPC 1 assumes for $c = 1$ that $\bar{u}_1$ can be any piecewise-constant input trajectory that satisfies the constraints of Eq. (26), but assumes that $\bar{u}_2 = \bar{h}_2(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, whereas Safeness Index-I-DLEMPC 2 assumes that $\bar{u}_1 = \bar{h}_1(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, but that $\bar{u}_2$ can be any piecewise-constant input trajectory that satisfies the constraints of Eq. (26)). Therefore, all m controllers may be feasible (i.e., Eqs. (26g)–(26h) may be satisfied in Safeness Index-I-DLEMPC j by the nominal trajectory of Eq. (1) under $\bar{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, and the assumed control actions in Eqs. (26d)–(26e)), but Eqs. (26g)–(26h) may not be satisfied for the nominal system of Eq. (1) under the trajectories $\bar{u}_{1,c}^*, (t|t_k) \ldots, \bar{u}_{m,c}^*(t|t_k)$, $t \in [t_k, t_{k+N})$ (this trajectory is denoted by $\tilde{x}^{tot}$ in the following) returned by the set of m Safeness Index-I-DLEMPC's at iteration c since that was not a condition required for feasibility of any of the m Safeness Index-I-DLEMPC's. Nevertheless, iteration $c+1$ is not guaranteed to be feasible unless $\tilde{x}^{tot}$ meets the constraints of Eqs. (26g)–(26h). Therefore, satisfaction of those constraints by the control actions returned at iteration c should be checked before a new iteration is performed. If Eqs. (26g)–(26h) are not satisfied by $\tilde{x}^{tot}$ and $c > 1$, the solution from iteration $c-1$ should be implemented (this implementation strategy ensures that the solution from iteration $c-1$ causes Eqs. (26g)–(26h) to be met or iteration c would not have been performed). If Eqs. (26g)–(26h) are not satisfied by $\tilde{x}^{tot}$ and $c = 1$, then $\bar{h}(x(t_k))$ should be implemented (the solution to the m Safeness Index-I-DLEMPC's should not be implemented because satisfaction of Eqs. (26g)–(26h) by $\tilde{x}^{tot}$ is required for the closed-loop stability results in the next section). This gives the following implementation strategy of the Safeness Index-I-DLEMPC design:

1. At t_k, all m Safeness Index-I-DLEMPC's receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2 ($c = 1$).
2. An attempt is made to solve all m Safeness Index-I-DLEMPC optimization problems. If $c = 1$, Safeness Index-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+r}))$, $\forall\, t \in [t_{k+r}, t_{k+r+1})$, $z \in \{1, \ldots, m\}$ but $z \neq j$, $r = 0, \ldots, N-1$. If $c > 1$, Safeness Index-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{u}_{z,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$ but $z \neq j$. If all m Safeness Index-I-DLEMPC's are feasible, go to Step 3. Else, go to Step 4.
3. Evaluate whether $V(\tilde{x}^{tot}(t)) \leq \rho_e$ and $S(\tilde{x}^{tot}(t)) \leq S_{TH}$, $\forall\, t \in [t_k, t_{k+N})$. Also, evaluate whether the iteration termination conditions are met (e.g., the objective function evaluated for $\tilde{x}^{tot}$ and $\bar{u}_{i,c}^*(t|t_k)$, $i = 1, \ldots, m$, $t \in [t_k, t_{k+N})$ fails to improve between two iterations). If Eqs. (26g)–(26h) are not satisfied by $\tilde{x}^{tot}$ or the iteration termination condition is met, go to Step 4. Else, any information required for evaluating the iteration termination condition (e.g., the objective function value) is stored, and go to Step 5 ($c \leftarrow c+1$).
4. If $c > 1$, implement $[\bar{u}_1^*(t_k|t_k) \;\ldots\; \bar{u}_m^*(t_k|t_k)] = [\bar{u}_{1,c-1}^*(t_k|t_k) \;\ldots\; \bar{u}_{m,c-1}^*(t_k|t_k)]$. Else, implement $[\bar{u}_1^*(t_k|t_k) \ldots \bar{u}_m^*(t_k|t_k)] = [\bar{h}_1(x(t_k)) \;\ldots\; \bar{h}_m(x(t_k))]$. Go to Step 6.
5. Safeness Index-I-DLEMPC j receives the optimal solutions $\bar{u}_{z,c-1}^*(t|t_k)$, $z = 1, \ldots, m$, $z \neq j$, $t \in [t_k, t_{k+N})$, for $j = 1, \ldots, m$. Go to Step 2.
6. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

3.2.1. *Feasibility and closed-loop stability analysis for the Safeness Index-I-DLEMPC implementation strategy*

Theorem 2 provides sufficient conditions under which the implementation strategy of the Safeness Index-I-DLEMPC maintains closed-loop stability of a nonlinear process.

Theorem 2. *Consider the system of Eq.* (1) *in closed-loop under the implementation strategy (Steps 1–6) of the Safeness Index-I-DLEMPC based on a controller $\bar{h}(x)$ that satisfies the conditions of Eq.* (2)*. Let $\epsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ satisfy Eqs.* (16) *and* (8)*. If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho_e$ and $N \geq 1$ where $\rho_{\min}$ is defined as in Eq.* (9) *and where the compact set $\Omega_{\rho_{\min}}$ satisfies Eq.* (17)*, then the closed-loop state $x(t)$ of Eq.* (1) *is guaranteed to enter the safety zone in finite time when $x(t_0) \in \Omega_\rho$, to be bounded within Ω_ρ at all times, and to be ultimately bounded in $\Omega_{\rho_{\min}}$.*

Proof. The proof consists of two parts. In Part 1, we demonstrate that the inputs applied to the process at every sampling time have characterizable properties. In Part 2, we demonstrate that this sequence of characterizable inputs guarantees the results of Theorem 2.

Part 1. At each sampling time, according to the implementation strategy of the Safeness Index-I-DLEMPC, either $\bar{h}(x(t_k))$ is implemented on the process, or a feasible solution to all m Safeness Index-I-DLEMPC's (i.e., a solution satisfying Eqs. (26b)–(26i) in Safeness Index-I-DLEMPC i, $\forall\, i = 1, \ldots, m$) is implemented that ensures $V(\tilde{x}^{tot}) \leq \rho_e$ and $S(\tilde{x}^{tot}) \leq S_{TH}$ from Step 3 of the implementation strategy (feasibility of Safeness Index-I-DLEMPC's 1 to m ensures that each implemented input $\bar{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+1})$, $i = 1, \ldots, m$, satisfies Eqs. (26c) and (26i) because satisfaction of these constraints depends only on the value of $\bar{u}_j^*(t|t_k)$ calculated by the controller and is not affected by the values of $u_z^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$). When $c = 1$, there is no guarantee that a feasible solution to Eq. (26) exists in any of the m Safeness Index-I-DLEMPC's when Eq. (26h) is applied (however, a feasible solution $\bar{u}_{i,1}^*(t|t_k) = \bar{h}_i(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, is guaranteed for Safeness Index-I-DLEMPC i, $i = 1, \ldots, m$, when Eq. (26h) is not applied because this manipulated input trajectory satisfies Eq. (26c) from Eq. (2), it satisfies Eq. (26g) when combined with the manipulated input trajectories of Eq. (26d) by Eq. (10) when $\rho_{\min} \leq \rho_e$, and it trivially satisfies Eq. (26i)). When $c > 1$, each iteration performed is guaranteed to have a feasible solution. To show this, it is noted that if iteration c is attempted, then $\bar{u}_{i,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, met Eqs. (26c) and (26i) from feasibility of those constraints at iteration $c-1$ and ensured that Eqs. (26g)–(26h) were satisfied by the nominal solution of Eq. (1) under $\bar{u}_{i,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, by Step 3 of the Safeness Index-I-DLEMPC implementation strategy. At iteration c, Safeness Index-I-DLEMPC j sets $\bar{u}_{z,c}^*(t|t_k) = \bar{u}_{z,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$, by Eq. (26e) (the input trajectory for the prior iteration except for $\bar{u}_{j,c-1}^*(t|t_k)$). Therefore, $\bar{u}_{j,c}^*(t|t_k) = \bar{u}_{j,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, is a feasible solution to Safeness Index-I-DLEMPC j because it is guaranteed to satisfy all constraints in Eq. (26) at iteration c since it satisfied them at iteration $c-1$ (even when the constraint of Eq. (26h) is applied). When any of the m Safeness Index-I-DLEMPC's is infeasible for $c = 1$, $\bar{h}(x(t_k))$ is implemented, and Proposition 1 holds. Thus, whether a feasible solution to the Safeness Index-I-DLEMPC's is implemented or $\bar{h}(x(t_k))$, the implemented solution is characterizable and closed-loop stability of a nonlinear system under such control actions can be analyzed.

Part 2. We will now prove the three results of Theorem 2. First, we prove that the Safeness Index-I-DLEMPC implementation strategy guarantees that the closed-loop state will enter the safety zone in finite time whenever $x(t_k) \in \Omega_\rho$ but $S(x(t_k)) > S_{TH}$. At each sampling time that $S(x(t_k)) > S_{TH}$ and a feasible solution to the m Safeness Index-I-DLEMPC's meeting the conditions checked in Step 3 of the Safeness Index-I-DLEMPC implementation strategy is implemented on the process, the constraint of Eq. (26i) is applied in each of the m Safeness Index-I-DLEMPC's. Summing these constraints gives Eq. (18a), and the results developed through Eqs. (18)–(24) in the proof of Theorem 1 hold, showing that $V(x(t_{k+1})) < V(x(t_k))$. Alternatively, if $\bar{h}(x(t_k))$ is applied at t_k when $S(x(t_k)) > S_{TH}$, then by Proposition 1, $V(x(t_{k+1})) < V(x(t_k))$. This indicates that at each sampling time that $S(x(t_k)) > S_{TH}$, the implementation strategy of the Safeness Index-I-DLEMPC drives $x(t)$ from a Lyapunov level set to one with a lower upper bound on the Lyapunov function. The state will either enter the safety zone before it enters $\Omega_{\rho_{\min}}$ or will be driven to $\Omega_{\rho_{\min}}$ (contained within the safety zone from Eq. (17)) in finite time. We next prove that the closed-loop state remains bounded in Ω_ρ at all times under the Safeness Index-I-DLEMPC implementation strategy. When a feasible solution to the Safeness Index-I-DLEMPC is implemented on the process, this solution satisfies the constraint of Eq. (26g) for $\tilde{x}^{tot}$ and/or the constraint of Eq. (26i). When the constraint of Eq. (26i) is applied (regardless of whether the constraint of Eq. (26g) is simultaneously applied), the analysis from the prior paragraph indicates that Eq. (24b) holds and therefore, $V(x(t)) \leq V(x(t_k))$, $\forall\ t \in [t_k, t_{k+1})$, so that the state cannot leave Ω_ρ within Δ if $x(t_k) \in \Omega_\rho$. If Eq. (26g) is applied but Eq. (26i) is not (i.e., $x(t_k) \in \Omega_{\rho_e}$, $t_k < t_s$, and $S(x(t_k)) \leq S_{TH}$), then utilizing Propositions 2 and 3, Eqs. (16) and (26g), and Step 3 of the implementation strategy, we conclude that Eq. (25) holds with $\tilde{x}^{tot}$ replacing $\tilde{x}^m$ and that $x(t) \in \Omega_\rho$, $\forall\ t \in [t_k, t_{k+1})$, if $x(t_k) \in \Omega_{\rho_e}$. If $\bar{h}(x(t_k))$ is implemented on the process and Eq. (8) holds, then Eqs. (18)–(24) hold and Eq. (24b) shows that $x(t)$ cannot leave Ω_ρ in Δ if $x(t_k) \in \Omega_\rho$. Therefore, under the implementation strategy of the Safeness Index-I-DLEMPC, the implemented control action at t_k ensures that $x(t) \in \Omega_\rho$, $\forall\ t \in [t_k, t_{k+1})$, whenever $x(t_k) \in \Omega_\rho$ and therefore, $x(t) \in \Omega_\rho$ throughout the length of operation if $x(t_0) \in \Omega_\rho$.

Finally, we prove that the closed-loop state is ultimately bounded in $\Omega_{\rho_{\min}}$ when $t_k > t_s$. In this case, either Eq. (26i) holds (if a feasible solution to the Safeness Index-I-DLEMPC is implemented) or $\bar{h}(x(t_k))$ is implemented. In both cases from the analysis above, $V(x(t_{k+1})) < V(x(t_k))$ for $x(t_k) \in \Omega_\rho/\Omega_{\rho_s}$. Once $x(t_k) \in \Omega_{\rho_s}$, then by definition of $\Omega_{\rho_{\min}}$, the closed-loop state will not leave $\Omega_{\rho_{\min}}$.

Remark 2. An ethylene oxidation process example from [11] was examined under a centralized Safeness Index-based LEMPC and under both iterative and sequential Safeness Index-based DLEMPC's. The results (see [12]) indicate that the two distributed designs may offer improved computation times compared to the centralized design while maintaining the state in the safety zone and improving economic performance compared to steady-state operation.

Acknowledgments

Financial support from the US National Science Foundation and the US Department of Energy is gratefully acknowledged. Fahad Albalawi acknowledges financial support from Taif University, Saudi Arabia.

References

[1] J. Wang, F. Yang, T. Chen, S.L. Shah, An overview of industrial alarm systems: Main causes for alarm overloading, research status, and open problems, IEEE Trans. Autom. Sci. Eng. 13 (2016) 1045–1061.
[2] N.G. Leveson, G. Stephanopoulos, A system-theoretic, control-inspired view and approach to process safety, AIChE J. 60 (2014) 2–14.
[3] F. Albalawi, H. Durand, P.D. Christofides, Process operational safety using model predictive control based on a process Safeness Index, Comput. Chem. Eng. 104 (2017) 76–88.
[4] P.D. Christofides, R. Scattolini, D. Mũnoz de la Peña, J. Liu, Distributed model predictive control: A tutorial review and future research directions, Comput. Chem. Eng. 51 (2013) 21–41.
[5] A.N. Venkat, I.A. Hiskens, J.B. Rawlings, S.J. Wright, Distributed MPC strategies with application to power system automatic generation control, IEEE Trans. Control Syst. Technol. 16 (2008) 1192–1206.
[6] H.K. Khalil, Nonlinear Systems, third ed., Prentice Hall, Upper Saddle River, New Jersey, 2002.
[7] S.S. Jogwar, M. Baldea, P. Daoutidis, Dynamics and control of process networks with large energy recycle, Ind. Eng. Chem. Res. 48 (2009) 6087–6097.
[8] D. Mũnoz de la Peña, P.D. Christofides, Lyapunov-based model predictive control of nonlinear systems subject to data losses, IEEE Trans. Automat. Control 53 (2008) 2076–2089.
[9] M. Heidarinejad, J. Liu, P.D. Christofides, Economic model predictive control of nonlinear process systems using Lyapunov techniques, AIChE J. 58 (2012) 855–870.
[10] P. Mhaskar, J. Liu, P.D. Christofides, Fault-Tolerant Process Control: Methods and Applications, Springer-Verlag, London, England, 2013.
[11] F. Özgülşen, R.A. Adomaitis, A. Çinar, A numerical method for determining optimal parameter values in forced periodic operation, Chem. Eng. Sci. 47 (1992) 605–613.
[12] F.A. Albalawi, Safe Model Predictive Control Formulations Ensuring Process Operational Safety, Doctoral Dissertation, University of California, Los Angeles, 2017.